دو فصلنامه علمی
مطالعات فقه اسلامی و مبانی حقوق
سال چهاردهم/ شماره چهل و دوم/ پاییز و زمستان ۱۳۹۹
۲۶۱-۲۸۳

Biannual journal of
Studies of Islamic Jurisprudence and Basis of Law
Vol, 14/ No, 42/ Fall & Winter 2021
261-283

گستره جرم جاسوسی اقتصادی و صنعتی با نگاهی به قانون ۱۹۹۶ کنگره ایالات متحده آمریکا*

سید متین محسنی**

چکیده

جاسوسی اقتصادی و صنعتی به جمع‌آوری اطلاعات اقتصادی یک کشور در مورد کشور دیگر تعریف گردیده است. وضعیت اقتصادی یک کشور، اهمیت بسزایی در امنیت ملی آن دارد که جاسوسی اقتصادی و صنعتی می‌تواند این مهم را هدف قرار دهد. اهداف این جاسوسی شامل جمع‌آوری اطلاعات در مورد تولید ناخالص، ارقام نرخ تورم، تخصیص بودجه برای دفاع، هزینه‌های پژوهش و توسعه ملی و گسترش صنایع مهم مانند الکترونیک، هوافضا، و بیوتکنولوژی می‌شود. در طول دوران جنگ سرد سرویس‌های اطلاعاتی و ضد جاسوسی در اهداف سیاسی و نظامی متمرکزشده بودند که تغییر اساسی درروند جاسوسی ایجاد گردید. جاسوسی اقتصادی و صنعتی به گزینه‌ای جذاب برای کشورهایی که اغلب متحد هستند، تبدیل‌شده است. تحمیل هزینه‌های سنگین جاسوسی اقتصادی و صنعتی بر اقتصاد آمریکا، ضعف قوانین مدنی در مبارزه با این موضوع و ناتوانی دادستان‌ها در استفاده مؤثر از سایر قوانین کیفری، کنگره را به این تصمیم واداشت که جاسوسی اقتصادی را تبدیل به جرم فدرال و قانون جاسوسی اقتصادی را در سال۱۹۹۶، تصویب کند.

کلید واژه‌ها: جاسوسی اقتصادی و صنعتی، اسرار تجاری، جرم جاسوسی، سرویس‌های اطلاعاتی، قانون جاسوسی اقتصادی۱۹۹۶.

---

* تاریخ دریافت مقاله: ۱۳۹۸/۱۰/۳۰ـ تاریخ پذیرش مقاله: ۱۳۹۹/۰۸/۲۸ـ نوع مقاله: علمی، ترویجی.

** دانشجوی دکتری جامعه المصطفی ﷺ العالمیه نمایندگی خراسان/
matin.mohseni@outlook.com

مقدمه

ما در جهانی زندگی می‌کنیم که در آن سلامت اقتصادی ملت‌ها و رقابت تجاری، عمدتاً به واسطه توانایی در توسعه تجارت و به دست آوردن منافع حاصل از نوآوری‌های علم و فناوری، تعیین می‌گردد. چنان‌که ادامه پیشرفت اینترنت و فناوری‌های نوین منجر به تغییر شکل زندگی ما شده و برای رقابت اقتصادی راه‌های سریع‌تر و کارآمدتر در انجام معاملات را ایجاد کرده است.

این واقعیت باعث افزایش جرایم اقتصادی گردیده است که تأثیر آن انکارناپذیر است. اتصال از طریق اینترنت، مفهوم مرزها و صلاحیت قضایی را با یک چالش باورنکردنی در مبارزه با این مسئله مواجه ساخته است.گروه‌های سازمان‌یافته جنایتکاران به راحتی می‌توانند مرتکب جرایم اقتصادی شده و از ضمانت اجرای قانونی جلوگیری کنند. مبارزه با این پدیده در توانایی یک کشور نیست، بلکه مستلزم افزایش همکاری میان نهادهای عدالت کیفری جهانی است.(Nasheri, ۲۰۰۵: ۳۵)

برای درک بیشتر از چگونگی فناوری اطلاعات، مقررات، قوانین و تعامل جهانی‌شدن برای مدیریت موفق، رقابت بین پیشرفت اقتصادی و فرصت‌های جنایی مورد نیاز است. انقلاب در فناوری اطلاعات تغییر اساسی در جوامع ایجاد کرده و این روند در آینده همچنان قابل پیش‌بینی خواهد بود. توسعه فناوری اطلاعات باعث تغییرات بی‌سابقه اقتصادی و اجتماعی گردیده که همچنان دارای ابعاد تاریک می‌باشند. فناوری‌های جدید مفاهیم حقوقی را به چالش کشیده‌اند. اطلاعات و ارتباطات به راحتی در سراسر جهان جریان دارد. دیگر در این روند مرزهای طولانی وجود ندارد. مجرمان به طور فزاینده‌ای در مکان‌هایی غیر از جای‌هایی که اقدامات مؤثرشان را ایجادمی کنند، قرار دارند. عصر اطلاعات امروز نیاز به رقابت در معاملات تجاری یک اساس جهانی است و به اشتراک‌گذاری اطلاعات حساس بر طرف‌های هم‌فکر در حالی است که حفاظت از اطلاعات مذکور در برابر رقبا، خرابکاران، مشتریان، و دولت‌های خارجی صورت می‌گیرد. قانونگذاران به طور فزاینده به تصویب قوانین کیفری برای ایجاد سیاست‌های اقتصادی و اجتماعی در خصوص استفاده و انتشار تکنولوژی متوسل می‌شوند. بسیاری بیم آن دارند که پیشرفت‌های فناوری در حال ساخت، شرکت در جاسوسی اقتصادی و صنعتی را آسان‌تر و ارزان‌ترکند.(Ibid:۳۶)

در اقتصاد جهانی، تفاوت کمتری بین نیاز به حفاظت از منافع دولت و نیاز به حفاظت از منافع تجاری وجود دارد. وضعیت اقتصادی یک کشور، بخش بزرگی از امنیت ملی آن را می‌سازد. این وضعیت اقتصادی بستگی به توانایی یک کشور به رقابت مؤثر در بازار جهانی دارد. جرایم جاسوسی صنعتی و اقتصادی جرایم جدی هستند، به این علت که

آثار آن‌ها در امنیت ملی کشورها ظاهر می‌گردد. بنابراین هم شرکت‌ها و هم قوانین اجرایی به طور یکسان در به دست آوردن کنترل جرم جاسوسی صنعتی و اقتصادی که تأثیر عظیمی بر سودآوری دارد، مشکل‌دارند. اگرچه راه‌حل‌های مدنی ممکن است به جبران خسارت حقوق بزه‌دیدگان بپردازد، اما راه‌حل‌های کیفری غالباً ضمانت اجرایی مطمئن و مجازات کافی و بازدارندگی از فعالیت‌های غیرقانونی دارد.

در ایالات‌متحده، کنگره به طور مستمر به گسترش و تقویت قوانین کیفری برای جلوگیری از جاسوسی صنعتی و اقتصادی پرداخته است، اما با این‌حال، قوانین داخلی به طور معمول به قلمرو خاص محدودشده است. این مشکل ظاهراً از آنجا ناشی می‌شود که مقامات ایالات‌متحده با مشاهده اقتصاد این کشور، شروع به تمرکز بر شکل جدید از جرم کرده‌اند که آثار زیانباری بر اقتصاد این کشور داشته است. کنگره هم برای مبارزه با این آثار قانون جاسوسی اقتصادی را تصویب کرد.

این قانون، اگرچه نسبتاً جدید است، اما دور از مفاهیم بین‌المللی است. بنابراین، راه‌حل برای مشکلات مطرح‌شده بایستی توسط قوانین بین‌المللی و با تصویب یک قانون آیین دادرسی مشترک صورت گیرد. این مقاله طیف گسترده‌ای از موارد جاسوسی صنعتی و اقتصادی را که هر دو به عنوان یک جرم و به عنوان یک مسئله امنیت ملی و بین‌المللی است به بحث و بررسی می‌گیرد.(Fialka, ۱۹۹۷: ۲۰)

۱. کلیات و مفهوم‌شناسی

درواقع جاسوسی جزء جرایم علیه امنیت دانسته می‌شود و کشورها در قوانین داخلی‌شان آن را مورد جرم انگاری قرار می‌دهند. حقوق‌دانان تعاریف زیادی را از جاسوسی ارائه کرده‌اند:

> جاسوسی عبارت است از گردآوری پنهانی و غیرقانونی اطلاعات مرتبط به امور سیاسی، نظامی یک کشور.(عالی‌پور، ۱۳۹۳: ۱۸۶)

این تعریف، به جاسوسی اقتصادی و صنعتی اشاره نکرده است و از این‌جهت ناقص است. در حقوق ایران بین حقوق‌دانان اختلاف است در اینکه موضوعات مورد جاسوسی شامل اسرار سیاسی و نظامی می‌گردد و یا اسرار اقتصادی و صنعتی نیز می‌گردد. برخی معتقدند شامل اسرار اقتصادی و صنعتی نیز می‌شود و برخی دیگر آن را محدود به اسرار سیاسی و نظامی تنها می‌دانند.[۱](مجیدی،۱۳۸۶: ۱۱۹)

---

۱. البته بایستی توجه داشت که منشأ این اختلاف در حقیقت به قانون مجازات مصوب ۱۳۷۰ ذیل ماده ۵۰۱ برمی‌گردد. هرچند قانون بزه‌های نیروهای مسلح مصوب ۱۳۸۲ به این مطلب دربند (ج) ماده ۲۴ تصریح دارد که اسرار شامل نظامی، سیاسی، امنیتی، اقتصادی و یا صنعتی می‌گردد.

در قانون مجازات جدید فرانسه(مصوب ۱۹۹۴) دامنه موضوع جاسوسی علاوه بر جاسوسی نظامی، سیاسی شامل جاسوسی اقتصادی و صنعتی نیز می‌گردد. بنابراین طبق این قانون تلاش‌های بعضی از افراد در جهت تحصیل و جمع‌آوری اطلاعات صنعتی و اقتصادی به دلیل حفظ موقعیت کشور در رقابت‌های صنعتی و اقتصادی نیز مشمول عنوان جاسوسی می‌گردد. حال آنکه در قانون سابق این کشور چنین چیزی وجود نداشت.(همان: ۱۲۹-۱۳۳)

علاوه بر اضافه نمودن مورد مذکور به این تعریف، بایستی ویژگی حساس اطلاعات را نیز به آن اضافه کرد. در خصوص تعیین مصادیق جاسوسی و مراحل آن همیشه اختلاف وجود داشته است. فارغ از گستردگی مفهوم و مصادیق جاسوسی، غالباً قانون‌گذاران جرم را به دو رفتار که عبارت است از جمع‌آوری اطلاعات و ارائه آن به دشمن منحصر ندانسته‌اند و معتقدند که مراحل سه‌گانه جاسوسی،[1] موجب نشده است جرم‌انگاری منتظر حصول نتیجه باشد، بلکه به صرف وجود هریک از مراحل جرم محقق شده است.

کشورها در طول تاریخ قبل از مواجهه نظامی همواره با حربه جاسوسی به مصاف هم رفته‌اند و در این میان جاسوسی را کلید تأمین امنیت دانسته‌اند. به عنوان‌مثال آمریکا با این هدف و با تصویب قانون امنیت ملی در سال ۱۹۴۷، سازمان خبرگیری مرکزی(سی. آی. ای) را تأسیس کرد که وظیفه اصلی آن جمع‌آوری و تحلیل اطلاعات و ارائه گزارش به دولت آمریکاست. جاسوسی هرچند به دلیل مغایرت با امنیت ملی دارای چهره منفی و سرزنش‌آمیز است، اما در چهره‌ای دیگر با تعابیری چون خبرگیری یا کسب اطلاع از کشورهای دیگر برای تأمین امنیت ملی، قابل توجیه و حتی ضروری است.(عالی‌پور، ۱۳۹۳: ۱۸۷-۱۸۸)

جاسوسی هرچند عمدتاً توسط سازمان‌های دولتی صورت می‌گیرد و در این میان جاسوسی‌های کشورهایی نظیر ایالات‌متحده و اتحاد جماهیر شوروی در دهه هشتاد قرن بیستم میلادی، این دوران را به دهه جاسوسی معروف کرده است، اما این جرم در کشورهای مختلف و توسط افراد و سازمان‌های گوناگون نیز ارتکاب می‌یابد. به ویژه با رایانه‌ای شدن امور و تجهیز مراکز دولتی حساس به رایانه و اینترنت، احتمال وقوع جاسوسی نسبت به گذشته به شدت افزایش‌یافته است. امروزه جاسوسی اقتصادی و صنعتی به یکی از فعالیت‌های اصلی سرویس‌هایی اطلاعاتی تبدیل‌شده است بنا به برخی

۱. شناسایی و تعیین اطلاعات مورد نیاز، جمع‌آوری اطلاعات و بالاخره تجزیه و تحلیل اطلاعات جمع‌آوری‌شده که نهایتاً منجر به هدف اصلی جاسوسی یعنی ارائه اطلاعات به مسئولان یک دولت یا شرکت بیگانه می‌گردد.

گزارش‌ها شرکت‌های بزرگ در سطح جهان که نوآوری انجام می‌دهند، دائماً در معرض جاسوسی قرار می‌گیرند که خسارت‌های ناشی از این جاسوسی شامل ارقام بسیار بزرگ می‌گردد و معمولاً شرکت‌ها از افشای موارد جاسوسی که درنتیجه باعث پائین آمدن سهام آن‌ها می‌گردد، خودداری می‌کنند.(صادقی، ۱۳۸۷: ۷۶)

۱. ۱. ابهام در تعریف جاسوسی اقتصادی و صنعتی

در ارتباط با این مسئله که جاسوسی اقتصادی و صنعتی جز ء کدام دسته از جرایم قرار می‌گیرد، از لحاظ جرم شناختی، برخی شک و تردیدهای را برانگیخته است، لذا برخی معتقدند با توجه اینکه جرایم یقه‌سفیدی شامل انواعی از جرایم غیر خشونت‌آمیز می‌گردد و از طرفی این جرایم در موقعیت‌های تجاری و برای به دست آوردن سود بیشتر ارتکاب می‌یابد. به دلیل وجود این خصوصیت معتقدند که جاسوسی اقتصادی و صنعتی جزء جرایم یقه‌سفیدی است.(Nasheri, ۲۰۰۵: ۳)

اصطلاح جرم یقه‌سفید ابتدا توسط ادوین ساترلند در جریان یک سخنرانی در انجمن جامعه‌شناسی آمریکا مورد شناسی قرار گرفت. در حقیقت این اصطلاح برای نخستین بار توسط وی ابداع گردید. ساتر لند جرم یقه‌سفید را به عنوان «جرمی که توسط فرد محترم و دارای موقعیت اجتماعی بالا و در ارتباط با شغل ارتکاب می‌یابد» تعریف نمود.(بنسون و سیمپسون، ۱۹۵۴: ۳۶)

آقای نجفی ابرندآبادی می گوید:

> ادوین ساترلند، در اواسط قرن بیستم، پس از مطالعه جرم شناختی بزهکاری چند بنگاه، شرکت و مؤسسه اقتصادی، مالی، تولیدی، خدماتی و بانکی آمریکایی به این نتیجه رسید که ارتکاب جرم و تکرار جرم در فرایند فعالیت‌های این اشخاص و مدیران و صاحبان آن‌ها، در واقع امری رایج است، لیکن به لحاظ گونه و شیوه ارتکاب جرم، سیاست‌های مساعدت و اغماض آمیزی نهادهای پلیسی، قضایی،صنفی در قبال آنان، روانشناسی این افراد که در خویشتن خویش، خود را مجرم یا ناقض قانون تلقی نمی‌کنند و بنابراین در سطح جامعه و در برابر عدالت کیفری رفتار و واکنش عادی از خود نشان می‌دهند بالاخره به لحاظ عدم حساسیت مشتریان و مصرف‌کنندگان و به طورکلی افکار عمومی نسبت به این طبقه از جامعه، یا شاکی ندارد یا کمتر کشف می‌شود و یا در جوامع قضایی، صنفی کمتر محکوم می‌گردد و درنهایت در آمار جنایی اثر اندکی از بزهکاری ظاهری و قضایی آن‌ها به چشم می‌خورد.(همان: ۱۲)

ساترلند نتایج مهمی را از مطالعه جرایم یقه‌سفیدی به دست آورد که خودش آن‌ها را به صورت ذیل بیان کرد:

۱. جرایم یقه‌سفیدان به مثابه پیامد حضور فرد در تجارت یا شغلی مشخص ظهور می‌یابند؛
۲. این جرایم بیشتر در محیط‌های صنعتی ارتکاب می‌یابند؛
۳. در میان حوزه‌های مختلف صنعت، برخی شرکت‌ها جرایم بیشتری را مرتکب می‌شوند.(سیمپسون و ویزبرد، ۱۹۵۴: ۳۳)

شباهت‌های زیادی بین جرایم یقه‌سفید و جاسوسی صنعتی و اقتصادی وجود دارد و این را می‌توان در بیان *ساترلند* نیز مشاهده کرد. می‌توان گفت که جاسوسی اقتصادی و صنعتی در این دسته از جرایم قرار می‌گیرند. البته بایستی به نکته توجه داشت که جاسوسی اقتصادی و صنعتی در بیشتر موارد توسط سازمان‌ها و دولت‌ها انجام می‌شود بااین‌حال در برخی موارد می‌تواند توسط فرد یا افراد نیز انجام شود. از سویی در بیان ویژگی جرایم یقه‌سفیدان می‌توان گفت که بسیاری از جرایم یقه‌سفیدها به سختی تحت پیگرد قرار می‌گیرند، چرا که مرتکبان آن مجرمان حرفه‌ای هستند و تلاش می‌کنند فعالیت‌هایشان را مخفی کرده و از طریق یک سری اقدامات پیچیده انجام دهند. این ویژگی‌ها در جاسوسی اقتصادی و صنعتی نیز مشاهده می‌شود.

ممکن است برخی این‌گونه استدلال کنند که شما در بحث قبلی جاسوسی اقتصادی و صنعتی را جزء جرایم علیه امنیت دانستی، حال‌آنکه جاسوسی اقتصادی و صنعتی اساساً یک رقابت در عرصه بین‌المللی محسوب می‌گردد به ویژه اگر آن را جزء جرایم یقه‌سفیدان بدانیم. اگرچه این حرف جای تأمل دارد و منطقی است، اما از آنجا که در بسیاری از موارد جاسوسی اقتصادی و صنعتی مستقیماً امنیت کشورها را نشانه می‌رود، بلکه بالاتر در بیشتر موارد شامل اطلاعات حساس نظامی و اقتصادی می‌گردد که می‌تواند به راحتی امنیت یک کشور را به خطر بیندازد، لذا نمی‌تواند صرفاً جنبه رقابتی داشته باشد.(Schweizer, ۱۹۹۳: ۵)

با وجود اینکه بسیاری از دانشمندان علوم اجتماعی اذعان کرده‌اند که جاسوسی اقتصادی به ویژه در عصر دیجیتال یک مشکل بزرگ است، با این‌حال، این موضوع کمتر در شاخه‌های علوم اجتماعی، به ویژه جرم‌شناسی و جامعه‌شناسی مورد توجه قرارگرفته است. با توجه به آثار زیانباری که جاسوسی اقتصادی و صنعتی بر اقتصاد کشورها دارد و می‌تواند زیرساخت‌های اقتصادی و صنعتی را هدف قرار دهد، می‌طلبد که توجه کافی به این مسئله صورت گیرد، بنابراین ما نخست در خصوص تعریف و سپس به گستره جاسوسی صنعتی و اقتصادی بپردازیم.

۱. ۲. جاسوسی اقتصادی و صنعتی

در خصوص جاسوسی اقتصادی و صنعتی تعریف‌های متعددی مطرح است که در اینجا به چند مورد از این تعاریف بسنده می‌کنیم. ابتدا به تعریف جاسوسی اقتصادی می‌پردازیم و سپس جاسوسی صنعتی را تعریف نموده و در نهایت مقایسه‌ای در شباهت‌ها و تفاوت‌های این دو نوع جاسوسی را بررسی خواهیم کرد.

تعریفی که جنبه‌های مختلف و جهات گوناگون و تا حدودی قطعی‌تر جاسوسی اقتصادی را بیان می‌کند، مربوط به سازمان اطلاعات امنیت کانادا[۱] است. با توجه به CSIS جاسوسی اقتصادی عبارت است از:

> عمل غیرقانونی، سری، قهری یا درگیر شدن در فعالیت فریبنده با بهره‌گیری از طرح یک دولت خارجی، برای دسترسی غیرمجاز به اطلاعات اقتصادی، همانند اطلاعات اختصاصی و یا فناوری، برای برتری اقتصادی.

با توجه به این تعریف می‌توان گفت که اطلاعات اقتصادی عبارت است از جمع‌آوری اطلاعات مربوط به تجارت که شامل اطلاعات فناوری، مالی، تجاری اختصاصی و اطلاعات دولتی می‌گردد و همین‌طور اطلاعات اقتصادی همانند اطلاعات در مورد تولید ناخالص ملی، ارقام نرخ تورم، تخصیص بودجه برای دفاع، هزینه‌های پژوهش و توسعه ملی که معمولاً این اطلاعات از طرق غیرقانونی به دست می‌آیند.(Gallagher ۱۹۹۸)

یکی دیگر از تعاریف جاسوسی اقتصادی مربوط به قانون جاسوسی اقتصادی در ایالات‌متحده آمریکا است. این قانون یکی از معدود شکل‌های قانون مصوب برای سرکوب جاسوسی اقتصادی در این کشور است که طبق این قانون، مفهوم مهم در ارتباط با جاسوسی اقتصادی مربوط به جاسوسی اطلاعات است. تعریفی که این قانون از جاسوسی اقتصادی ارائه می‌کند در حقیقت مستلزم گردآوری، همکاری و مشارکت در عملیات طراحی‌شده توسط یک دولت خارجی و استفاده غیرمجاز از اطلاعات است.(Keithly & Ferris ۲۰۰۲)

به نظر می‌رسد بایسته‌ترین تعریف درعین‌حال که پیچیده و غامض نیست و از سویی دارای ویژگی‌هایی است که بیانگر انواع از رفتارهای که نقش مهم در ایجاد جاسوسی اقتصادی دارند نیز می‌گردد، این تعریف است: «جاسوسی اقتصادی عبارت از جمع‌آوری اطلاعات اقتصادی توسط یک کشور در مورد کشور دیگر».(Nasheri,۲۰۰۵:۱۶)

امروزه این نوع جاسوسی به دو طریق رخ می‌افتد:

۱.Canadian Security Intelligence Service.

أ) یک کارمند ناراضی اسرار تجاری یک شرکت را برای به دست آوردن سود مالی خودش یا به قصد آسیب زدن به شرکت، سرقت می‌کند.

ب) برای یک شرکت رقیب یا یک کشور خارجی اسرار را سرقت می‌کند که هدفش کسب سود بیشتر برای خودش است.

سرقت‌هایی که بدین شیوه در این حوزه‌ها اتفاق می‌افتد، گاهی پیچیده هستند، همانند هک کامپیوتر، جاسوسی دستگاه‌های اطلاعاتی، زمانی هم شامل سرقت‌های پیش‌پاافتاده مانند سرقت اسناد، عکس‌برداری و کپی‌برداری می‌گردد.(ibid:۷)

در عرصه بین‌المللی انواع زیادی از جاسوسی وجود دارد که برخی از متداول‌ترین آن‌ها شامل جاسوسی از رقبا، فروشندگان، محققان، مشاوران اطلاعات تجاری، مطبوعات و سازمان‌های دولتی می‌شود. مستخدمان جاسوسی اغلب افراد با استعداد و با مهارت تحلیلی بالا هستند. این اشخاص در جمع‌آوری مقادیر قابل‌توجهی از اطلاعات و ترکیب آن‌ها با یکدیگر مهارت زیادی دارند. برای سرقت اطلاعات و انجام جاسوسی برخی از کشورها به جای سازمان‌های بزرگ یا سازمان‌های اطلاعاتی به استخدام افراد می‌پردازند[1] و برخی دیگر از کشورها به استخدام گروهی از اشخاص برای نفوذ در شرکت‌های خارجی و سرقت ایده‌ها اقدام می‌کنند.(Fialka, ۱۹۹۷: ۱۸)

جاسوسی اقتصادی به یکی از شیوه‌های ذیل انجام می‌شود:

> اسکن اسناد طبقه‌بندی‌شده تجاری، استفاده از نرم‌افزارهای داده‌کاوی و جستجو از طریق اینترنت پرسرعت برای به دست آوردن اطلاعات، بررسی بایگانی‌ها با سازمان‌های نظارتی، استراق سمع در پایانه‌های خطوط هوایی و پروازها، سرقت لپ‌تاپ‌ها، نفوذ به اتاق فرمان از یک مکان نزدیک با استفاده از تجهیزات تجسسی، حضور در دادگاه محاکمه رقبا، حتی در مواردی گشتن زباله‌دانی‌ها برای به دست آوردن اطلاعات.(Gomes, ۱۹۹۹)

کسانی که جاسوسی اقتصادی را سازماندهی می‌کنند به طور ویژه این دسته از اطلاعات را هدف قرار می‌دهند.

در خصوص جاسوسی اقتصادی در ایالات‌متحده آمریکا پرونده‌های زیادی وجود دارد که در بیشتر موارد آن سازمان‌های اطلاعاتی این کشور قادر به تشخیص نبوده‌اند. به

---

۱. چنان که نظیر این مسئله را می‌توان در دوران جنگ سرد مشاهده کرد. جاسوسی‌های فراوان که بین ایالات‌متحده آمریکا و شوروی در دهه هشتاد قرن بیستم میلادی، اتفاق افتاد، این دوران را به دهه جاسوسی معروف کرد. سازمان اطلاعاتی همانند C.I.A و K.G.B که اقدام به استخدام افراد بانفوذ برای جاسوسی می‌کردند؛ البته با این تفاوت که در این دوران غالب جاسوسی‌ها مربوط اطلاعات و اسرار نظامی بود.

عنوان مثال یک شرکت در ایالات متحده پیشنهاد یک قرارداد الکترونیکی بین‌المللی را از دست داد. بعد از گذشت مدت زمان کوتاهی، متوجه شد که یک سازمان اطلاعاتی اروپا به نحوی قیمت‌گذاری را رهگیری می‌کرده است. سازمان اطلاعاتی مذکور این اطلاعات مهم را در اختیار شرکت دیگری که در نهایت برنده مزایده شد، قرارداد.

در حادثه دیگر، سازمان اطلاعات و امنیت کانادا تعدادی از خدمه پرواز ایر فرانس را شناسایی کرد که درواقع عوامل سرویس اطلاعاتی فرانسه بودند. این‌ها نمونه‌های کوچکی از جاسوسی اقتصادی است که در کشورهای غربی ارتکاب می‌یابد با توجه به اینکه امروزه دهکده جهانی شکل‌گرفته است این جاسوسی محدود به کشورهای غربی نیست و می‌تواند در هر کشوری رخ دهد، آنچه حائز اهمیت و مهم به نظر می‌رسد، توجه به این نوع جاسوسی است که نشان‌دهنده یک امر حیاتی و در حال گسترش است.(Boadle, ۱۹۹۴)

با وجود برخی از اشتراکات جاسوسی اقتصادی و صنعتی از لحاظ تئوری، اما این دو از شرایط منحصربه فردی برخوردار هستند. وزارت دادگستری ایالات‌متحده آمریکا جاسوسی صنعتی را این‌گونه تعریف کرده است:

> جاسوسی صنعتی عبارت است از انجام فعالیت به وسیله یک فرد، دولت خارجی یا توسط یک شرکت خارجی با حمایت مستقیم دولت خارجی علیه یک شرکت خصوصی ایالات‌متحده با هدف دستیابی به اسرار تجاری.

همان‌طوری که ملاحظه می‌گردد این تعریف نه فعالیت‌های نهادهای خصوصی را تحت‌الشعاع قرار می‌دهد و نه تلاش‌های قانونی برای دست‌آوردن اطلاعات تجاری مفید همانند اطلاعات تجاری موجود در اینترنت را؛ اما نکته تأمل‌برانگیز در این تعریف این است که اساساً تشخیص این نوع جاسوسی‌ها که آیا تحت حمایت دولت‌های خارجی انجام می‌شود یا نه بسیار مشکل است. حقیقتاً تفاوتی میان جاسوسی اقتصادی و صنعتی ازلحاظ تئوریک مشاهده نمی‌شود و اشتراکاتشان به قدری زیاد است که نمی‌توان قائل به تفکیک شد، اما با این وجود، اشتراکات هریک از شرایط منحصر فردی برخوردار هستند. شاید مهم‌ترین تفاوت میان جاسوسی اقتصادی و صنعتی این باشد که اولی به دنبال دستیابی به اطلاعات به صورت عام است که از این نظر شامل جاسوسی صنعتی نیز می‌گردد، بنابراین امروزه جاسوسی صنعتی شامل جمع‌آوری اطلاعات در مورد صنایع مهم مانند الکترونیک، هوافضا، دفاع و یا بیوتکنولوژی می‌گردد. به دست آوردن چنین اطلاعاتی توسط کشور خارجی می‌تواند به صورت مستقیم یا غیرمستقیم به بهره‌وری نسبی و یا موقعیت رقابتی آن کشور در عرصه اقتصادی کمک کند.(Gallagher ۱۹۹۸)

۱. ۳. هزینه‌های سنگین جاسوسی اقتصادی و صنعتی بر اقتصاد آمریکا

ازآنجا که این تحقیق در پی تبیین جرم جاسوسی اقتصادی و صنعتی در حقوق آمریکا است، لذا بایستی پیامدهای این جرایم را در فضای این کشور مورد بررسی قرار دهیم. در خصوص جرایم اقتصادی مردم آمریکا در دوره‌های زمانی مختلف دیدگاه‌های متناقض داشته‌اند. گاهی این جرایم را به عنوان یک مسئله کوچک و زمانی به عنوان یک بحران بزرگ می‌نگریستند. در اواسط دهه هشتاد میلادی، این موضوع همگانی بوده است که ناشی از بحران مالی بود که در آن زمان وجود داشت. برخی از نویسندگان آمریکایی معتقدند که به طورمعمول در ایالات‌متحده توجه عظیم ملی بر جرایم مرسوم و متداول است، به ویژه جرایم خشونت‌آمیز. مثالی که عنوان می‌کنند این است که یک ارزیابی از عملیات امنیتی شرکت‌های داخلی و روش‌های حفاظت شان نشان می‌دهد که دیدگاه کلی این شرکت‌ها در موضوع امنیت فقط حمایت از مردم و منافع ملموس فیزیکی است، نه حمایت از اطلاعات حساس اقتصادی. با توجه به چنین رویکردی سنتی نسبت به امنیت، طبیعتاً این شیوه مناسب برای حفاظت از اطلاعات در مقابل جاسوسی اقتصادی و صنعتی نیست.

مثالی که برای این منظور بیان می‌کنند این است که بسیاری از شرکت‌های این کشور حتی از دست دادن اطلاعات اقتصادی و تجاری مهم که توسط سرویس‌های اطلاعاتی خارجی به سرقت می‌روند را تشخیص نمی‌دهند.(Nasheri, ۲۰۰۵: ۳)

با توجه به گزارش اداره تحقیقات فدرال آمریکا(اف. بی. آی.) تخمین زده می‌شود که ارزش مالی جرم یقه‌سفیدان در ایالات‌متحده بیشتر از ۳۰۰ بیلیون دلار در سال برسد، که از میان سهم جاسوسی اقتصادی و صنعتی ۵۹ میلیارد دلار در سال است.(قبولی درافشان و همکاران، ۱۳۹۲: ۱۰۶) با وجود این، حفاظت از اطلاعات اقتصادی و تجاری به طور فزاینده‌ای در عرصه رقابت صنعتی جهان مهم محسوب می‌گردد. از آغاز دهه ۱۹۹۰ میلادی، قدرت فناوری اطلاعات دارای رشد تصاعدی بوده است و در نتیجه ابزار مهم و قدرتمند برای سرقت و انتقال اطلاعات حفاظت‌شده، محسوب می‌گردد. این تکامل فناوری در جوامع غربی انواع خاصی از فعالیت‌های مجرمانه و خرابکارانه از قبیل جاسوسی اقتصادی و صنعتی را تسهیل کرده است. توجه و تمرکز بر جاسوسی اقتصادی نشان‌دهنده یک باور اساسی است و آن اینکه این مسئله اهمیت گسترده‌تر از نگرانی‌های امنیت ملی دارد. علاوه بر این، عدم توافق در مورد تعریف جرایم اقتصادی و جرایم با تکنولوژی‌های پیشرفته منجر به کمبود اطلاعات در این خصوص شده است.

در ایالات‌متحده آمریکا شرکت‌های تجاری و افراد، بخش عمده‌ای از فعالیت‌های بین‌المللی جاسوسی صنعتی را تشکیل می‌دهند. به عنوان مثال در آمریکا در صنایع

دفاعی ۵۸٪ از جاسوسی صنعتی توسط شرکت‌ها و افراد انجام می‌شود، درحالی‌که تنها ۲۲٪ از آن مربوط به حمایت دولت‌های خارجی می‌گردد، طبق گزارش سالانه F.B.I به کنگره، اهمیت طبقه‌بندی طرفین درگیر در جاسوسی اقتصادی و صنعتی بر دو گروه بیان شده است؛ اول ملل متفق و دوست که مرتکب جاسوسی علیه یکدیگر می‌شوند. در حقیقت در جهان جاسوسی اقتصادی، هیچ روابط دوستانه واقعی وجود ندارد و آن هم عمدتاً به دلیل این واقعیت است که کشورهایی که در فعالیت‌های جاسوسی درگیر و در حال رقابت‌اند برای یک پله سعود از نردبان بازار جهانی تلاش می‌کنند. (Moyer ۱۹۹۴:۱۸۲)

دوم، کشورهای در حال توسعه که به شدت در این تجارت پرسود درگیر هستند، به ویژه با تحولات اساسی که بعد از فروپاشی شوروی و به وجود آمدن قدرت‌های نوظهور پدید آمده است. در زمان اتحاد جماهیر شوروی دولت‌های کمونیستی در تلاش برای پیشی گرفتن از غرب مبادرت به جاسوسی اقتصادی و صنعتی می‌کردند. عوامل اطلاعاتی کشورهای بلوک شرق، منابع قابل‌توجهی را برای جمع‌آوری اطلاعات در مورد کشورهای دیگر یا عناصر وابسته به آن، اختصاص می‌دادند و به جمع‌آوری اطلاعات ضد جاسوسی برای محافظت در برابر فعالیت‌های اطلاعاتی کشورهای دیگر می‌پرداختند. مشکل جاسوسی اقتصادی و صنعتی به طور قابل‌توجهی از زمان پایان جنگ سرد افزایش‌یافته است.(ibid)

بر اساس گزارش سالانه کنگره در مدیریت سرمایه‌گذاری مستقیم منابع خارجی و فعالیت‌های جاسوسی علیه شرکت‌های دارای فناوری‌های حیاتی ایالات‌متحده آمده است؛ سازمان اطلاعاتی یک کشور متحد می‌خواست از عملیات جاسوسی که یک کارمند ایالات‌متحده در حال انجام آن بود فرار کند. این کارمند اسناد طبقه‌بندی‌شده نظامی را می‌خواست در اختیار این سازمان قرار دهد که در یک عملیات ضد جاسوسی دستگیر شد. در مورد دیگر چند شهروند که در حال سرقت تکنولوژی ساخت لوله تفنگ و همین‌طور برنامه‌های طراحی‌شده برای یک سیستم شناسایی شرکت آمریکایی بودند و می‌خواستند به یک پیمانکار دفاعی در کشور خودشان تحویل دهند، دستگیر شدند.(ibid)

یکی از نویسندگان آمریکایی در سال ۱۹۹۳ کتابی در موضوع جاسوسی اقتصادی و صنعتی نوشت. وی در این کتاب بیان کرد که چگونه دوستان آمریکا از این کشور جاسوسی می‌کنند. وی در حقیقت با نوشتن این کتاب شروع به آگاه کردن مردم و سیاستمداران این کشور کرد. اشوایزر در این کتاب یک‌چشم‌انداز وسیع از جاسوسی اقتصادی و صنعتی را از مقام ارشد سازمان اطلاعات فرانسه نقل می‌کند. آقای پیرماریون

مدت طولانی مقام بلندپایه سازمان اطلاعات فرانسه بود. وی در خصوص جاسوسی اقتصادی و صنعتی اظهار می‌دارد:

> من فکر می‌کنم که شما بایستی به صورت بسیار واضح مسائلی را که از یک متحد مخفی‌شده‌اند از مسائلی که مخفی نشده‌اند جدا کنید. این بسیار واضح است که شما زمانی متحد هستید که بخش‌های خاص داشته باشید، من از تسلیحات صحبت می‌کنم. فکر می‌کنم مسائل دیپلماتیک به طورمعمول جایی که بایستی شما سعی به جمع‌آوری اطلاعات نکنید، اما در تمام زمینه‌های دیگر، اتحاد موجود نباید کشورها را از وجود رقابت منع کند. حتی در دوران جنگ سرد، رقابت‌های اقتصادی بین کشورها از سطح سیاسی ـنظامی به سطح اقتصادیـ تکنولوژیکی در حال حرکت بود. در اقتصاد، ما رقیب هستیم نه متحد. فکر می‌کنم حتی در دوران جنگ سرد گردآوری اطلاعات در موضوعات اقتصادی، تکنولوژیکی و صنعتی از یک کشور با آنکه متحد هستید سازگار با این واقعیت که شما متحد هستید، نیست.(Schweizer۱۹۹۳:۹)

اشوایزر از کشورهایی نام می‌برد که متحدان استراتژیک ایالات‌متحده آمریکا محسوب می‌گردند. کشورهای همانند فرانسه، اسرائیل، آلمان، کره‌جنوبی و ژاپن. وی به این مطلب تصریح می‌کند که این کشورهای به ظاهر دوست چگونه اقدام به جاسوسی اقتصادی و صنعتی علیه ایالات‌متحده در ۴۵ سال گذشته کرده‌اند. افشاسازی اشوایزر مورد پذیرش دولت ایالات‌متحده آمریکا در ماه اوت ۱۹۹۶ قرار گرفت، هنگامی‌که سازمان اطلاعات مرکزی(CIA) هم‌پیمانان ایالات‌متحده از جمله فرانسه و اسرائیل را که درگیر در جاسوسی اقتصادی و صنعتی شده بودند، متهم کرد. اتهام در نتیجه یک لیست که توسط مرکز اطلاعات ملی ضد جاسوسی گردآوری‌شده بود، ارائه گردید، این لیست شامل آن دسته از کشورهایی می‌شود که باور بر این است به طور گسترده در جاسوسی اقتصادی درگیر هستند.(ibid)

سازمان اطلاعات مرکزی اتهام جاسوسی اسرائیل از ایالات‌متحده را در پاسخ به سؤالات هیئت اطلاعات مجلس سنا گردآوری کرد. اولین‌بار بود که دولت ایالات‌متحده به افشاسازی جاسوسی اقتصادی علیه اسرائیل می‌پرداخت. این فاش‌سازی در مورد اسرائیل تا حدودی روابط دو کشور را وارد مرحله جدیدی کرد آن‌هم با توجه به روابط نزدیک تاریخی بین ایالات‌متحده و اسرائیل.

گزارش‌های سازمان شامل گواهی یک متخصص دفتر حسابداری عمومی امنیت ملی، بنام دیوید ای کوپر، می‌گردید. او گزارش داد که با توجه به تحقیقات دفتر فدرال و سرویس‌های اطلاعات برخی از نزدیک‌ترین متحدان ایالات‌متحده به طور فعال به دنبال

به دست آوردن اطلاعات طبقه‌بندی‌شده و فنی ایالات‌متحده از طریق ابزارهای غیرمجاز هستند. سازمان همچنین مشخص کرد که فعالیت‌های سرویس‌های اطلاعاتی کشورهای خارجی علیه تکنولوژی‌های حیاتی ایالات‌متحده صورت گرفته است و این فعالیت‌ها تهدید قابل‌توجهی علیه امنیت ملی محسوب می‌گردد. اگرچه این گزارش تنها از واژه‌هایی مانند کشور A و کشور B استفاده کرده است، اما توصیف این کشورها و حوادث نشان می‌دهد که کشور A اسرائیل و کشور B فرانسه است.(Ibid)

بر اساس این گزارش، اسرائیل تهاجمی‌ترین عملیات جاسوسی را علیه ایالات‌متحده و هر متحد آن انجام داده است. این گزارش اعلام کرد که اطلاعات نظامی طبقه‌بندی‌شده و فناوری‌های حساس نظامی مهم‌ترین اهداف سرویس‌های اطلاعاتی اسرائیل است. این گزارش مستند همچنین نشان می‌دهد که چگونه فرانسه یک تلاش تهاجمی گسترده را علیه ایالات‌متحده آغاز کرده است. کاهش تنش‌های شرق و غرب در اواخر دهه ۱۹۸۰ و نزدیک دهه ۱۹۹۰ سرویس‌های اطلاعاتی فرانسه را قادر به تخصیص منابع بیشتر برای جمع‌آوری اطلاعات حساس اقتصادی و فناوری آمریکا ساخت.

در همین خصوص یک سازمان دولتی فرانسه اظهار داشت که هدایت این فعالیت‌ها، هدف قرار دادن اطلاعات دفاعی ایالات‌متحده مانند برنامه جنگ، نیست، بلکه به دنبال فناوری اطلاعات این کشور است. گردآوری اطلاعات مربوط به فعالیت‌های جاسوسی فرانسه چیزی جدیدی برای جامعه اطلاعاتی ایالات‌متحده محسوب نمی‌گردد. به گفته مقامات سازمان سیا و اف. بی. آی. فعالیت‌های جاسوسی فرانسه تا آنجا پیش رفته است که این کشور اقدام به گذاشتن دستگاه شنود در صندلی‌های خطوط هوایی ایر فرانس برای گوش دادن مکالمات بازرگانان آمریکایی و همچنین به جستجو در اتاق‌های هتل آن‌ها پرداخته‌اند.(Hirst and Breslan, ۱۹۹۵: ۳۴)

۱. ۴. افزایش جاسوسی اقتصادی و صنعتی از شرکت‌های آمریکایی

تعدادی از عواملی که به افزایش جاسوسی اقتصادی در سال اخیر، کمک کرده است، افزایش دسترسی و استفاده از تکنولوژی کامپیوتر است. سودآوری زیاد و فقدان منابع تحقیق و پیگرد کننده منجر به چنین جاسوسی گردیده است. با افزایش اهمیت عوامل اقتصادی در تعریف امنیت ملی کشورها، این مسئله باعث گسترش سرقت اطلاعات اقتصادی و صنعتی در سال‌های اخیر شده است.(Nelson &Anders ۱۹۹۹)

بخش عمده سرانه در ایالات‌متحده آمریکا را سرمایه مالکیت فکری از قبیل اختراعات ثبت‌شده تشکیل می‌دهد. در این کشور جاسوسی اقتصادی و صنعتی به صورت گسترده و مکرر در مناطق با بیشترین مراقبت تکنولوژیکی، تحقیقی و فعالیت‌های توسعه‌ای رخ

می‌دهد. بر اساس گزارش‌های اف.بی.آی. حداقل ۲۳ دولت خارجی به طور فعال اسرار تجاری شرکت‌های ایالات‌متحده را هدف قرار داده‌اند.

در مطالعاتی که توسط اف. بی. آی. انجام‌شده است، همچنان نشان می‌دهد که ۱۷۳ کشور جهان از ایالات‌متحده جاسوسی کرده‌اند. این گزارش نشان می‌دهد که حدود ۱۰۰ کشور منابع زیادی را صرف به دست آوردن فناوری اطلاعات از ایالات‌متحده کرده‌اند که از این ۱۰۰ کشور، ۵۷ کشور در عملیات‌های متعدد ضد شرکت‌های آمریکایی وارد عمل شده‌اند.(Schweizer, ۱۹۹۶)

با توجه به گزارش اف. بی. آی. کشورهایی که به طور گسترده‌ای در فعالیت‌های جاسوسی علیه شرکت‌های آمریکایی درگیر بوده‌اند، عبارت‌اند از فرانسه، اسرائیل، چین، کوبا، هلند، بلژیک، آلمان، ژاپن، هند و چند کشور اسکاندیناوی. نمونه‌هایی از مناطقی که هدف جاسوسی قرارگرفته‌اند، شامل سیلیکون والی، دیترویت، کارولینای شمالی، دالاس، بوستون، واشنگتن دی سی و منطقه پنسلوانیا–نیوجرسی، جایی که در آن بسیاری از شرکت‌های دارویی و بیوتکنولوژی این کشور قرار دارند. به گفته برخی از کارشناسان آمریکایی، سیلیکون والی منطقه‌ای است که هدف بیشترین حملات قرارگرفته است. آن‌ها اظهار داشته‌اند صنایع که معمولاً آماج بیشترین هدف قرار می‌گیرند عبارت‌اند از صنایع هوافضا، بیوتکنولوژی، نرم‌افزار و سخت افرارکامپیوتر، حمل‌ونقل و تکنولوژی موتوری، تجهیزات نظامی، مخابراتی، تحقیق انرژی، مواد و پوشش‌های پیشرفته(فناوری‌های به ویژه نانو ذرات و نانوتکنولوژی)، فناوری رادار گریز، لیزر و نیمه‌رساناها(اجسام که رسانا برای الکتریسیته می‌باشند) هستند.(Ibid)

قربانیان این جاسوسی در ایالات‌متحده شرکت‌های بزرگ همانند جنرال موتور، اینتل، لاکهید مارتین و هیوز ایر کرفت می‌باشند. علاوه بر موارد مذکور اطلاعات اختصاصی و محرمانه مانند اطلاعات لیست مشتریان، توسعه محصول، قیمت‌گذاری، آمار فروش، برنامه‌های بازاریابی، کارکنان، مزایده، تجزیه‌وتحلیل هزینه‌های تولید، اطلاعات و برنامه‌ریزی استراتژیک نیز هدف جاسوسی قرار می‌گیرند. تاکنون ژاپن، تایوان، چین، کره جنوبی، اتحاد جماهیر شوری سابق و جمهوری فدراسیون روسیه فعلی بیشترین منابع را برای سرقت فناوری از سیلیکون والی[1] اختصاص داده‌اند. در ایالات‌متحده آمریکا تقریباً

۱. یک نام مستعار برای بخش جنوبی منطقه خلیج سانفرانسیسکو در شمال کالیفرنیا در ایالات‌متحده است. در این منطقه بزرگ‌ترین شرکت‌های تکنولوژی جهان قرار دارد. در اصل این اصطلاح به تعداد زیادی از نوآوران تراشه سیلیکونی و تولیدکنندگان در این منطقه اشاره دارد، اما درنهایت به تمام بازرگانی با تکنولوژی پیشرفته در این منطقه، اشاره می‌کند. در حال حاضر به عنوان کنایه برای تکنولوژی‌های پیشرفته بخش اقتصادی آمریکا استفاده می‌شود.

هر شرکت بزرگ دارای یک اداره اطلاعات رقابتی است که برای کشف اسرار تجاری از رقبا طراحی‌شده است، برخی از شرکت‌های این کشور مانند موتورولا دارای واحدهای اطلاعاتی در سراسر جهان است.(King & Bravin, ۲۰۰۱)

۲. پایان جنگ سرد؛ تغییر در روند جاسوسی تا تصویب قانون جاسوسی اقتصادی

در این مبحث ما در پی آن هستیم که روند تغییر و چرخش جاسوسی از نظامی به جاسوسی اقتصادی و صنعتی را پس از دوران جنگ سرد بررسی کنیم و همین‌طور نشان دهیم که چگونه این روند باعث پیدایش یک دوره جدید شده است و اغلب کشورهای بزرگ صنعتی به این سمت روی آورده‌اند. در واقع، خلاف دوران جنگ سرد که رقابت تسلیحاتی مورد توجه بلوک شرق و غرب بود امروزه رقابت اقتصادی و صنعتی مورد توجه است.

۲. ۱. جاسوسی اقتصادی و صنعتی پس از دوران جنگ سرد

پس از دوران جنگ سرد سازمان‌های اطلاعاتی ـ از ناتو تا کا.گ.ب. و سازمان سیاـ به دنبال بازتعریف ساختارها و به عهده گرفتن نقش‌ها و عملکردهای جدید هستند. جاسوسی صنعتی و اقتصادی یک گزینه جذاب برای این سازمان‌ها است. برعکس دوران جنگ سرد که سرویس‌های اطلاعاتی و ضد جاسوسی در اهداف نظامی و سیاسی متمرکز بودند و موارد معمول جاسوسی در این دوران شامل فروش تکنولوژی نظامی توسط یک دانشمند آمریکایی به اتحاد جماهیر شوروی و یا به یکی از کشورهای اروپای شرقی می‌شد(Fraumann,۱۹۹۷) پس از جنگ سرد شرایط تغییر کرد. امروزه دخالت دولت‌ها در امور اقتصادی افزایش‌یافته است. تفکیک واقعی بین بخش خصوصی و دولتی دچار ابهام شده است. بازرگانان نقش دوگانه ایفا می‌کنند. طوری که تعدادی از آن‌ها به عنوان سیاستمدار و عده‌ای از سیاستمداران در هیئت‌مدیره شرکت‌ها به ایفای نقش می‌پردازند. در حقیقت با پایان جنگ سرد کشورها بر اجرای سیاست‌هایی متمرکز شدند که بتواند استانداردهای اقتصادی را در زندگی شهروندان افزایش دهند. امروزه برتری اقتصادی از نظر جایگاه همان اهمیت برتری نظامی در دوران جنگ سرد را دارد. ازاین‌رو است که جاسوسان در پایان جنگ سرد به بخش خصوصی برای انجام کارهای غیرقانونی روی آوردند. مطالعات انجام‌شده در این خصوص نشان می‌دهد که سالانه نزدیک به ۲۴ میلیارد دلار از مالکیت فکری شرکت‌های بزرگ به سرقت می‌رود.(Vaknin, ۲۰۰۲)

همان‌طوری که ذکر شد با سقوط کمونیسم، جامعه اطلاعاتی آمریکا مجبور به بازتعریف مأموریت و نقش خود در جهت پاسخگویی به واقعیت‌های جدید پس از جنگ

سرد شد. اشکال مختلف جاسوسی به تدریج در حال‌توسعه است. در حال حاضر فعالیت‌های جاسوسی عمدتاً معطوف به تمرکز روی فناوری، فرایند ساخت و دیگر اسرار تجاری است که گاهی اوقات استفاده دوگانه دارند، اما اغلب تنها کارکردهای غیرنظامی دارند. سرویس‌های اطلاعاتی کشورها حتی متحدان آمریکا به طور فزاینده‌ای منابع خودشان را به سرقت فناوری از این کشور اختصاص داده‌اند.(Keithly and Ferris ۲۰۰۲)

نمونه‌ها شواهد زیادی از این تغییر را می‌توان پس از دوران جنگ سرد مشاهده کرد که چگونه کشورها به جاسوسی اقتصادی و صنعتی روی آورده‌اند. برای مثال مدت کوتاهی پس‌از آنکه افسر CIA[۱] آمس در سال ۱۹۸۵ شروع به فروش اسرار به کا.گ.ب نمود، یک دانشمند به نام رونالد هافمن نیز شروع به فروش اطلاعات طبقه‌بندی‌شده ناچیز نمود. آمس در ازای ۲/۵ میلیون دلار، اسامی خبرچینان آمریکا در شوروی را در اختیار این کشور قرار دارد که براثر اطلاعات داده‌شده توسط او یازده جاسوس آمریکا در شوروی بین سال‌های ۱۹۸۵–۱۹۸۷ دستگیر و اعدام شدند که ازجمله آن‌ها ژنرال دیمیتری پولیاکوف افسر عالی‌رتبه سازمان اطلاعات شوروی بود.(صادقی ۱۳۸۷: ۷۹)

هافمن مدیر پروژه یک شرکت بنام ساینس اپلیکیشن[۲] ۷۵۰،۰۰۰ دلار از فروش برنامه‌های نرم‌افزاری پیچیده طرح توسعه دفاع استراتژیک که درواقع اطلاعات باارزش برنامه‌های هوافضای غیرنظامی بود، تحت یک قرارداد مخفی به شرکت‌های چندملیتی ژاپنی نیسان موتور[۳] الکترونیک میتسوبیشی،[۴] صنایع سنگین میتسوبیشی[۵] و صنایع سنگین ایشی کاواجیما‌ـحریما[۶] به دست آورد. آمس در یک پوشش خبری قابل‌توجه جانش را در ازای خیانتش از دست داد، با این‌حال، پرونده هافمن نشان‌دهنده آینده جاسوسی اطلاعات است. هرچند یکی برای مهم‌ترین رقیب نظامی آمریکا جاسوسی کرد و دیگری اطلاعات را به یک رقیب بزرگ اقتصادی این کشور فروخت.(Fialka,۱۹۹۷)

۲. ۲. گردآوری اطلاعات اقتصادی و جنگ جدید

امروزه استحکام اقتصادی و فنی، کلید قدرت و نفوذ هر کشوری است. گفتمان تجاری به عنوان حیاتی‌ترین شکل دیپلماسی جایگزین کنترل تسلیحاتی شده است.(Schweizer, ۱۹۹۶: ۱۳) سازمان‌های دولتی در حال حاضر نقش رو به جلو در

۱.Aldrich Rick Ames.
۲.Science Applications.
۳.Nissan Motor Company.
٤.Mitsubishi Electric.
٥.Mitsubishi Heavy Industries.
٦.Ishikawajima-Harima Heavy Industries.

جمع‌آوری اطلاعات محرمانه دارند. شاید مسئله تعجب‌آور در مورد این روند این است که مرتکبان جاسوسی اقتصادی و صنعتی اغلب متحدان یکدیگر هستند، به عنوان مثال کشورهای اروپای غربی نوعاً متحدان سنتی ایالات‌متحده آمریکا محسوب و دارای روابط دوستانه دیپلماتیک و فرهنگی می‌باشند، اما این کشورها به جاسوسی اقتصادی و صنعتی از ایالات‌متحده می‌پردازند. آن‌ها با دسترسی گسترده و آسان به اطلاعات این کشور نسبت به دشمنان سنتی ایالات‌متحده به راحتی می‌توانند اقدام به جاسوسی کنند، این در حالی است که سرویس‌های اطلاعاتی این کشور اغلب آموزش‌دیده‌اند. حتی در دوران جنگ سرد، کشورهای که به طور رسمی با ایالات‌متحده علیه شوروی متحد بودند به جاسوسی از شرکت‌های آمریکایی می‌پرداختند.

در واقع، جاسوسی اقتصادی توسط سرویس‌های اطلاعاتی متحدان، یک امری آشکار در میان بسیاری از متخصصان FBI و CIA در دوران جنگ سرد بود، اما سرویس‌های اطلاعاتی ایالات‌متحده این فعالیت‌ها را مخفی نگه می‌داشتند تا اطمینان حاصل کنند که سرویس‌های اطلاعاتی متحدان این کشور همچنان به جاسوسی در اتحاد جماهیر شوروی ادامه می‌دهند یا نه.(ibid: ۵)

در پایان این مبحث می‌توان گفت که همان‌طوری که رقابت‌های اقتصادی و صنعتی جایگزین رویارویی نظامی در بسیاری از امور جهان شده است، جاسوسی برای به دست آوردن تکنولوژی‌های حیاتی نیز همچنان به رشد خود ادامه خواهد داد و این روند در آینده می‌تواند تهدید جدی برای امنیت اقتصادی کشورها ایجاد کند.

۲. ۳. حمایت‌های قانونی از اسرار اقتصادی و تجاری در مقابل جاسوسی

حمایت از اسرار تجاری و اقتصادی درواقع ریشه در این تفکر دارد که انسان بایستی احترام به آزادی فردی، محرمانه بودن روابط، اخلاق متداول و رقابت عادلانه داشته باشد. قانون اسرار تجاری بیشتر از مفاهیم قرارداد و اعتماد نسبت به اموال ناشی می‌شود. چون اطلاعات به عنوان اسرار تجاری نگهداری می‌شوند و در برابر سوءاستفاده از آن حمایت قانونی صورت می‌گیرد. در حقیقت قانون اسرار تجاری جدید در ایالات‌متحده آمریکا توسط استانداردهای حقوق عرفی موردحمایت قرار می‌گیرد و آن را قابل‌احترام و اعتبار می‌سازد. در آمریکا صاحبان اسرار تجاری و اقتصادی از قرن هجدهم از قوانین عرفی حمایت می‌کردند و در همین راستا یک دادگاه در ماساچوست این حقوق را در محدوده اطلاعات محرمانه در سال ۱۸۳۷ به رسمیت شناخت.(Paine, ۱۹۹۱)

تئوری که از اسرار تجاری و اقتصادی حمایت می‌کند در حقیقت یک فرضیه مهم برای حفاظت از آن‌ها محسوب می‌گردد. به عنوان مثال کسانی که نوآوری و خلاقیت انجام می‌دهند و نیروی کار و تجهیزات و پول را در این راستا هزینه می‌کنند، اگر

حمایت‌های قانونی از آن‌ها صورت نگیرد و قانون به آن‌ها این تضمین را ندهد که درازای نوآوری می‌توانند سود لازم را ببرند، تمایلی برای انجام این کار از خودشان نشان نخواهند داد.

بر اساس همین تئوری است که قانون اسرار تجاری توسط سه سیاست مهم عمومی پشتیبانی می‌گردد؛ قانون اسرار تجاری برای حفظ اخلاق تجاری و اقتصادی به تاجران اطمینان می‌دهد که با حسن نیت وارد معاملات شوند، قانون اسرار تجاری کسانی را که اولین بار نوآوری‌شان را وارد بازار می‌کنند تضمین‌های لازم را به آن‌ها می‌دهد و آن‌ها را در این راستا تشویق می‌کند و در نهایت قانون اسرار تجاری جاسوسی اقتصادی و صنعتی را با حفظ حریم خصوصی صاحب اسرار تجاری، مجازات می‌کند.(Jager, ۱۹۹۶)

طبق حقوق کامن‌لو کارفرمایان حق مالکیت در اسرار تجاری‌شان را داشته‌اند و افشای اطلاعات محرمانه تخطی از رابطه اشتغال محسوب و شبه جرم بوده است. طبق ماده ۵۷۵ این قانون استفاده از اسرار تجاری در صورت وجود شرایط ذیل برای فرد می‌تواند مسئولیت‌آور باشد:

> ۱. اسرار را از طرق نامشروع به دست آورده است. ۲. استفاده یا افشاسازی با نقض تعهد امانی همراه باشد. ۳. اسرار تجاری را از ثالثی دریافت نموده و با علم به اینکه اطلاعات فوق، اسرار تجاری‌اند و نیز علم به اینکه ثالث از طریق نامشروع یا با نقض تعهد امانی، اطلاعات را به دست آورده است. ۴. اسرار تجاری را از شخص ثالثی دریافت نموده با علم به این‌که اطلاعات، اسرار تجاری است و ثالث اشتباهاً اسرار را فاش کرده است.(Restatements of Torts, sec. ۷۵۷ ۱۹۳۹)

قوانین جرایم کامپیوتری نیز سرقت اطلاعات اقتصادی، تجاری، کلاه‌برداری و اختلاس را مورد جرم‌انگاری قرار داده است. طبق این قوانین سرقت اطلاعات اقتصادی و تجاری چه در سطح ایالت‌ها و چه در سطح فدرال جرم محسوب و با مرتکب طبق قانون برخورد می‌گردید.(اسچب و اسچب دوم، ۱۹۹۹: ۲۹۴)

اگرچه قوانین مدنی و قوانین جرایم کامپیوتری و سایر قوانین حمایت از مالکیت فکری برای حفظ اسرار و اقتصادی پتانسیل مؤثر را ارائه می‌داد و برای حفظ اسرار تجاری شرکت‌ها و معاملات تجاری یک رویکرد دفاعی مؤثر را اتخاذ می‌کرد، اما با وجود این، ظرفیت سوءاستفاده از اسرار تجاری و اقتصادی همچنان رو به گسترش است. در آمریکا این وضعیت وجود داشت تا اینکه قانون جاسوسی اقتصادی تصویب شد.

۲. ۴. تصویب قانون جاسوسی اقتصادی

ناامید شدن و شکست راه‌حل‌های مدنی برای جلوگیری از سرقت اسرار تجاری و اقتصادی، ناتوانی دادستان‌ها در استفاده مؤثر از سایر قوانین کیفری و تلاش‌های مکرر دولت‌های خارجی برای به دست آوردن اسرار تجاری از شرکت‌های آمریکایی، باعث گردید که کنگره آمریکا سرقت اسرار تجاری و اقتصادی را به جرم فدرال تبدیل و قانون جاسوسی اقتصادی را در ماه اکتبر سال ۱۹۹۶ تصویب کند. (Economic Espionage Act of ۱۹۹۶)

نکته‌ای که در اینجا لازم است بیان شود بحث مربوط به صلاحیت رسیدگی جرم جاسوسی اقتصادی و صنعتی است. قبل از تصویب قانون جاسوسی اقتصادی، رسیدگی به این جرم در محدوده صلاحیت قوانین سرقت بود؛ اما بعد از تصویب قانون جاسوسی اقتصادی این صلاحیت به دادگاه‌های فدرال واگذار شد. صلاحیت دادگاه‌های فدرال در آمریکا هم توسط ماده دوم قانون اساسی این کشور بیان شده است و هم توسط قوانین موضوعه که کنگره تصویب می‌کند. طبیعتاً صلاحیت دادگاه‌های ایالتی نیز توسط قانون اساسی و قوانین موضوعه هر ایالات تعیین می‌گردد و اساساً می‌توان گفت که دادگاه‌های فدرال هنگامی به پرونده‌ها رسیدگی می‌کنند که متهمین به نقض قوانین کیفری فدرال متهم باشند.(اسچب، اسچب دوم، ۱۹۹۹: ۶۳)

بر اساس این قانون فعالیت مجرمانه توسط هر شخصی عمداً و با علم به اینکه این جرم، نفع به دولت خارجی، ابزار سودمند برای دولت خارجی یا عامل خارجی است، اقدام به:

۱. سرقت یا تصاحب، حمل، برداشتن، پنهان نمودن یا تحصیل از طریق خدمه و کلاهبرداری بدون اجازه مالک؛

۲. نسخه‌برداری، کپی‌برداری، حمل، عکس‌برداری، تخریب، انتقال، تحویل، ارسال پستی و ارسال پستی الکترونیک بدون اجازه مالک؛

۳. دریافت، خرید یا مالکیت اسرار تجاری، تصاحب یا انتقال مالکیت بدون اجازه دارنده؛

۴. شروع به جرم هریک از موارد فوق کند به اعمال مجازات‌های سنگین که در این قانون در نظر گرفته‌شده است، مواجه خواهد شد.

حبس ۱۰ سال و جریمه نقدی ۲۵۰ هزار دلاری برای اشخاص حقیقی و ۵ میلیون دلاری برای اشخاص حقوقی، این قانون در حقیقت با استفاده از اجرای مجازات‌های شدید بخشی از اهداف بازدارندگی در حمایت از جاسوسی اقتصادی و سرقت اسرار تجاری را محقق کرده است.(Economic Espionage Act of ۱۹۹۶ section ۱۸۳۱)

در حقیقت نیاز به قانون جاسوسی اقتصادی در آمریکا تجربه هایی است که این کشور در سرقت اسرار تجاری دارد. سرقت پروژه‌های چند میلیارد دلاری که برای نمونه می‌توان به یکی از آن‌ها اشاره کرد؛ دستگاه تجاری تصویرسازی تشدید مغناطیسی(MRI) که توسط ریموند دامدین اختراع گردید. سرقت این اختراع خسارت جبران‌ناپذیری به شرکت فانر[۱] وارد کرد. دکتر دامدین[۲] در مورد اینکه شرکتش چگونه مورد حمله رقبای خارجی قرار گرفت، اظهار داشت:

> یک شرکت خدماتی فاقد مجوز که خدمات تجهیزات پزشکی ارائه می‌کرد، مهندسین خدمات شرکت فانر را استخدام کرده، د رنتیجه به یک مجموعه کامل از طراحی مهندسی عالی مخفی و چندین نسخه از نرم‌افزارهای کپی‌رایت ما را به دست آورد... .(Damadian,۱۹۹۶)

وی معتقد بود که فقدان قانون در این خصوص باعث گردید که این مزیت ارزشمند از کنترل این شرکت خارج گردد. یکی از رقبای فانر، شرکت توشیبا نیز با فریب یک مهندس شرکت توانست داده‌های فنی به کار رفته بر روی محصولات فانر را به دست آورد. دامدین به زودی متوجه شد که توشیبا پرداخت تمام‌صورت حساب‌های حقوقی مهندس را منوط به مبارزه با فانر نموده است. این در حالی بود که فانر روش‌های نصب و راه‌اندازی مغناطیسی خودش را پشت درهای بسته نگهداری می‌کرد و در تلاش برای حفاظت از باارزش‌ترین تکنولوژی خودش بود.(ibid)

امروزه MRI صنعت چند میلیارد دلاری است. هرچند MRI اختراعی آمریکایی است، اما تنها دو شرکت از هشت شرکت فروشنده حتی در بازار آمریکا، آمریکایی هستند. فانر در حال حاضر به مراتب کوچک‌تر از نُه شرکتی است که در این صنعت فعالیت دارند. در بیان ویژگی این صنعت می‌توان اظهار داشت که بیشترین سود و هزاران شغل فنی با درآمد بالا توسط این اختراع ایجادشده است.(Fialka, ۱۹۹۶)

نتیجه‌گیری

جاسوسی اقتصادی و صنعتی مشکل بزرگی پس از دوران جنگ سرد است. همان طوری که در این نوشتار نشان داده شد، جاسوسانی که زمانی برای به دست آورد اطلاعات نظامی از کشورهای یکدیگر مشغول بودند، حالا به جاسوسی اقتصادی و صنعتی روی آورده‌اند. امروزه به خلاف گذشته که قدرت نظامی، برتری محسوب می‌گردید، استحکام اقتصادی و فنی، کلید قدرت و نفوذ هر کشوری است. سود

۱. Fonar.
۲. Damadian.

سرسام‌آوری که در جمع‌آوری اطلاعات اقتصادی و تجاری وجود دارد از طرفی افزایش اهمیت عوامل اقتصادی در تعریف امنیت ملی هر کشوری که اگر فاش گردد، امنیت آن به مخاطره جدی خواهد افتاد، جاسوسی اقتصادی و صنعتی را تبدیل به یک تجارت پررونق کرده است.

کشوری همانند ایالات‌متحده آمریکا که خود محصولات و تکنولوژی‌های جدید را در جهان توسعه و رهبری می‌کند، از جاسوسی اقتصادی و صنعتی سایر کشورهای غربی حتی نزدیک‌ترین متحدانش در امان نیست. داده‌های مالی و تجاری دولت و شرکت‌های بزرگ این کشور، دائماً توسط سرویس‌های اطلاعاتی کشورهای متحد به سرقت می‌روند، این در حالی است که اقتصاد این کشور کاملاً اطلاعات محور است. تجربه این کشور این مطلب را ثابت می‌کند که هیچ تجارتی مصون از جاسوسی اقتصادی نیست.

هر چند آمریکا تلاش‌هایی را از دهه ۱۹۹۰ میلادی در مبارزه با جاسوسی اقتصادی و صنعتی که منجر به تصویب قانون جاسوسی اقتصادی، در سال ۱۹۹۶ گردیده، آغاز کرده است، اما با رشد روزافزون تکنولوژی‌های نوین پیچیدگی روش‌های جاسوسی اقتصادی، بعید به نظرمی رسد که این قانون هم بتواند در مبارزه با این مسئله توفیق حاصل کند، هرچند این قانون در مقایسه با قوانین قبلی در برخورد با جاسوسی اقتصادی از استحکام لازم برخوردار است. آنچه کنگره را به سمت تصویب قانون جاسوسی اقتصادی هدایت کرد، معضلی بود که پس از جنگ سرد فراروی اقتصاد این کشور قرار دارد و آن جاسوسی نزدیک‌ترین متحدان این کشور است که حتی این روزها هم در خبرها می‌شنویم که فرانسه اقدام به جاسوسی و شنود مکالمات مقامات ایالات‌متحده یا بالعکس کرد.

منابع و مآخذ:

–ام اسچب، ام اسچب دوم، جان(۱۳۸۳)، ***حقوق جزا***، ترجمه امیر سماواتی پیروز، چ۱، تهران: مؤسسه فرهنگی انتشاراتی نگاه بینه.

–سیمپسون و ویزبرد سالی اس، دیوید(۱۳۹۲)، ***جرم‌شناسی جرایم یقه‌سفیدان***، ترجمه حمیدرضا دانش‌ناری و آزاده صادقی، چ۱، تهران: انتشارات مجد.

–صادقی، حسین میر محمد(۱۳۸۷)، *جرایم علیه آسایش عمومی*، چ۱، تهران: نشر میزان.
–عالی‌پور، حسن(۱۳۹۳)، حقوق کیفری فناوری اطلاعات، چ۲، تهران: انتشارات خرسندی.
–قبولی درافشان، مهدی، حمید رضا دانش ناری و علی ساعتچی(۱۳۹۲)، *مطالعه تطبیقی حمایت مدنی و کیفری از اسرار تجاری در نظام حقوقی ایران و آمریکا*، دو فصلنامه حقوق اقتصادی (دانش و توسعه سابق)، ش۴.
–مایل ال. بنسون وسالی اس. سیمپسون(۱۳۹۱)، *جرایم یقه‌سفیدان رویکردی فرصت مدار*، ترجمه اسماعیل رحیمی‌نژاد، چ۱، تهران: میزان.
–مجیدی، سید محمود(۱۳۸۶)، *جرایم علیه امنیت* «مطالعه تطبیقی جرایم جاسوسی، تبانی، محاربه و تروریسم در حقوق کیفری ایران و فرانسه»، چ۱، تهران: میزان.
– Boadle, Anthony. “Canada Spy-Catcher Says High-Tech Firms Targeted.” The Reuter European Business Report, ۱۳ April ۱۹۹٤.
– Damadian, Raymond. Testimony before the House Comm. on the Judiciary Subcomm. on Crime. Federal Document Clearing House, ۹ May ۱۹۹٦.
– Fialka, John J. “Stealing the Spark: Why Economic Espionage Works in America.” Wasington Quarterly ۱۹۹٦.
– Fraumann, Edwin. “Economic Espionage: Security Missions Redefined.” Public Administration Review, vol. ٥٧ (۱۹۹۷).
– Gallagher, Neil J. “Cybercrime, Transnational Crime, and Intellectual Property Theft: Hearing Before the J. Econ. Comm. ۱۰٥th Cong. ۲–٤,”۱۹۹۸. Retireved from: <http://www.wiu.edu/library/govpubs/guides/intellect.htm>.
– Gomes, Lee. “Upstart Linux Draws a Microsoft Attack Team.” Wall St. J. ۲۱ May ۱۹۹۹.
– Hirst, Michael, and Karen Breslan. “Closing the Deal, Trade Is the Main Focus of Bill Clinton’s Foreign Policy.” Newsweek, ٦ March ۱۹۹٥.
– Jager, Melvin F.Trade Secrets Law. New York: Clark Boardman Callaghan & Co,۱۹۹٦.
– Kaslow, Amy. “Behind White House Role as Pitchman for U.S. Firms.” Christian Science Monitor, ۲۸ March ۱۹۹٥.

– Keithly, David M. and Stephen P. Ferris. “U.S. Companies Exposed to Industrial Espionage; Point of View ”National Defense, vol. ۸۷ (۱ September ۲۰۰۲).
– King, Neil, Jr. and Jess Bravin. “Call It Mission Impossible, Inc. Corporate Spying Firms Thrive.” Wall St. J. ۳ July ۲۰۰۰.
– Moyer, Marc A. “Section ۳۰۱ of the Omnibus Trade and Competitiveness Act of ۱۹۸۸: A Formidable Weapon in the War Against Economic Espionage.” Northwestern Journal of International Law and Business, vol. ۱۵ (۱۹۹٤).
– Nelson, Emily, George Anders, and Raju Narisetti.“How Kodak, Fearing Theft of Trade Secrets, Mounted Its Own Sting.” Wall St. J. ۲۵ November ۱۹۹٦.
– Paine, Thomas. “The American Crisis.” In Heritage of American Literature Beginnings to the Civil War, edited by James E. Miller, Jr. For Worth, TX: Harcourt Brace Jovanovich Collage Publisher, ۱۹۹۱.
– Schweizer, Peter. Friendly Spies: How American Allies Are using Economic Espionage to Steal Our Secrets. New York: Atlantic Monthly Press, ۱۹۹۳.
– Vaknin, Sam. “Analysis: The Industrious Spies II.” United Press International, Financial News, ۱٤ May ۲۰۰۲.